UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/575,727	02/08/2007	Goran Selander	4147-155	1800

23117 7590 06/08/2009

NIXON & VANDERHYE, PC
901 NORTH GLEBE ROAD, 11TH FLOOR
ARLINGTON, VA 22203

EXAMINER	
PICH, PONNOREAY	
ART UNIT	PAPER NUMBER
2435	

MAIL DATE	DELIVERY MODE
06/08/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/575,727	SELANDER ET AL.	
	Examiner	Art Unit	
	PONNOREAY PICH	2435	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *13 April 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-32* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-32* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *13 April 2006* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *4/06*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Claims 1-32 are pending.

Information Disclosure Statement

As per the IDS submitted on 4/13/06, document 2003/188158 was struck out as not considered because there is no US Patent document with that serial number. Note that US PG publications have a serial number of 11 digits, not 10. The other documents were not considered because a copy of these documents was not provided to the Office as required by 37 CRF 1.98(a)(2).

Specification

It is unclear if the references cited in the last page of the specification and referred to in the rest of the specification are essential material or not and if applicant meant to incorporate these materials by reference or not. Note that essential material may not be incorporated by reference if the material is not a US patent or US patent application, see 37 CFR 1.57. Clarification by applicant is respectfully requested.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 1-32 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

1. Claim 1 recites "iteratively applying, whenever necessary, a predetermined one-way key derivation function…." Whenever necessary is a relative term and it is unclear what criteria are used to determine when it is necessary to iteratively apply a predetermined one-way key derivation function as recited in claim 1. Claims 16 and 31 are rejected as being indefinite for substantially similar reason.
2. "said one-way key derivation function" recited in claim 22 lacks antecedent basis. Applicant may have meant "said predetermined one-way key derivation function".
3. Claims 16-32 invoke 112, 6th paragraph via use of means plus function language. It is submitted that the disclosure as originally filed fails to adequately describe any structure corresponding to any of the means recited in these claims. As such, the metes and bounds of these claims cannot be determined.
4. Claim 32 is directed towards a security-key producing entity and recites that the entity comprises "means for iteratively applying a one-way key derivation function a given number of times starting from key information of a master key generation to derive key information of a predetermined key generation". This limitation is contradicts what is disclosed in the specification since this limitation essentially states that the key-producing entity derives key information of an older/predetermined generation using the key information from a subsequent/newer/master key generation. The specification on page 6 appears

to state the opposite. That is page 6 of the specification appears to state that the key-producing entity generates the newer/master key information using an older/predetermined key information. It is unclear if it is the specification that is incorrect or if it is the claim 32 which is written incorrectly.

5. Claims not specifically addressed are rejected due to dependency.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 16-32 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Claim 16 is directed towards an arrangement comprising means for distributing, means for replacing, and means for iteratively applying. As discussed above, the specification failed to disclose a corresponding structure for any of these recited means. As such, these elements are given the broadest, reasonable interpretation possible and in such an interpretation, it is submitted that each of these claimed elements could be interpreted to be directed towards software elements per se. As such, claim 16 appears to be directed towards software per se, which does not fall within any of the four statutory categories of invention and software by itself is incapable of achieving any functionality until interrelated with some form of hardware. For these reasons, claim 16 is not statutory. Claims 17-30 also appear to not be statutory because despite the

limitations further recited in these claims, each of the elements being claimed could still be interpreted as being directed towards software per se.

Claims 31 and 32 are also not statutory because each of the respective entities being claimed appear to also be directed towards software per se since the specification failed to disclose a corresponding structure for any of the means claimed in either claims and it would have been reasonable to interpret each of the claimed means as being software elements per se.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1, 5-19, 12-16, 20-24, and 27-32 are rejected under 35 U.S.C. 102(b) as being anticipated by Candelore (US 6,363,149).

Claims 1 and 16:

As per claim 16, Candelore discloses:

1. Means for distributing, at key update, key information of a new key generation from the key-producing side to the key-consuming side (col 4, lines 8-15 and col 9, line 25-col 10, line 27);

2. Means for replacing, on the key-consuming side, key information of an older key generation by the key information of the new key generation (col 6, lines 43-51 and col 9, line 25-col 10, line 27);
3. Means for iteratively applying, whenever necessary, a predetermined one-way key derivation function on the key-consuming side to derive key information of at least one older key generation from the key information of the new key generation (col 9, line 25-col 10, line 27 and Fig 5A).

Claim 1 is directed towards the method implemented using the arrangement of claim 16 and is rejected for much the same reasons.

Claim 31:

Candelore discloses:

1. Means for receiving, at key update, key information of a new key generation (col 4, lines 8-27 and col 9, line 25-col 10, line 27);
2. Means for replacing key information of an older key generation stored in said security-key consuming entity by the key information of the new key generation (col 6, lines 43-51 and col 9, line 25-col 10, line 27);
3. Means for iteratively applying, whenever necessary, a predetermined one-way key derivation function to derive key information of at least one older key generation from the key information of the new key generation (col 9, line 25-col 10, line 27 and Fig 5A).

Claim 32:

Candelore discloses:

1. Means for iteratively applying a one-way key derivation function a given number of times starting from key information of a master key generation to derive key information of a predetermined key generation (col 6, lines 43-51 and col 9, line 25-col 10, line 27 and Fig 5A); and
2. Means for distributing a representation of the derived key information to at least one key-consuming entity in the information environment for the purpose of secure communication (col 4, lines 8-27; col 7, line 36-col 8, line 3; and col 9, line 25-col 10, line 27).

Claims 5 and 20:

Candelore discloses wherein said means for iteratively applying a predetermined one-way key derivation function to derive key information of at least one older key generation is operable for enabling the key-consuming side to use any older key generation in the information environment even though one or more previous key updates have been missed (col 9, line 25-col 10, line 27 and Fig 5A).

Claims 6 and 21:

Candelore further discloses wherein the key-producing side comprises a key-issuing server issuing security key information to be shared by: at least one communication device and a provider of protected data for said at least one communication device (col 4, lines 8-27 and col 6, lines 42-51).

Claims 7 and 22:

Candelore further discloses wherein said at least one communication device comprises a group of devices, each of which comprises means for iteratively applying said one-way key derivation function, thereby enabling each group device with access to the new key generation to communicate also based on any older key generation (col 1, lines 5-10; col 7, lines 36-47; Fig 1; and Fig 5A).

Claims 8 and 23:

Candelore further discloses wherein group devices with access to the new key generation are enabled to share protected data also based on any older key generation (col 1, lines 5-10; col 7, lines 36-47; Fig 1; and Fig 5A).

Claims 9 and 24:

Candelore further discloses wherein the key-consuming side comprises said at least one communication device and said provider of protected data (col 1, lines 5-10; col 7, lines 36-47; Fig 1; and Fig 5A).

Claims 12 and 27:

Candelore further discloses wherein said means for iteratively applying a one-way key derivation function is operable for deriving key information that directly corresponds to a cryptographic key (col 9, line 25-col 10, line 27 and Fig 5A).

Claims 13 and 28:

Candelore further discloses means for transforming said derived key information into a cryptographic key (col 9, line 25-col 10, line 27 and Fig 5A).

Claims 14 and 29:

Candelore further discloses wherein said key-derivation function is based on a cryptographic hash function (col 9, line 25-col 10, line 27 and Fig 5A).

Claims 15 and 30:

Candelore further discloses wherein said security key information is used for Digital Rights Management in a digital content distribution system, on-line gaming, file sharing in a Local or Personal Area Network, store-and-forward applications or for securing on-line sessions (col 10, lines 5-27).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 2-3 and 17-18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Candelore (US 6,363,149) in view of Kaufman et al (US 5,483,598).

Claims 2 and 17:

Kaufman discloses means for generating, on the key-producing side, the key information of said new key generation by iteratively applying an instance of the predetermined one-way key derivation function starting from key information of a predetermined key generation (Fig 1B and col 3, lines 47-61).

At the time applicant's invention was made, it would have been obvious to one skilled in the art to modify Candelore's invention according to the limitations recited in

claims 2 and 27 in light of Kaufman's teachings. Note that while Candelore discloses of a key-producing side, he does not explicitly disclose how the key-producing side actually produce the key. It would have been obvious to modify Candelore's invention in the manner discussed because it would be nothing more than simple substitution of one known element for another to achieve predictable results. In this case, only the specific means for generating keys is replaced with another means for generating keys, but keys are still generated by the key-producing side.

Claims 3 and 18:

Candelore further disclose wherein said predetermined key generation is a master key generation (col 9, line 25-col 10, line 27 and Fig 5A).

Claims 4 and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Candelore (US 6,363,149) in view of Kaufman et al (US 5,483,598) in further view of Schneier ("Applied Cryptography, second edition").

Claims 4 and 19:

Kaufman discloses means for generating, on the key-producing side, the key information of said new key generation by applying a function of the predetermined one-way key derivation function starting from key information of any older key generation. (Fig 1B and col 3, lines 47-61). Further Schneier discloses the function being a trap-door function (p30).

At the time applicant's invention was made, it would have been obvious to one skilled in the art to modify Candelore's invention according to the limitations recited in claims 4 and 19 in light of Kaufman and Schneier's teachings. Note that while Candelore discloses of a key-producing side, he does not explicitly disclose how the key-producing side actually produce the key. It would have been obvious to modify Candelore's invention in the manner discussed because it would be nothing more than simple substitution of one known element for another to achieve predictable results. In this case, only the specific means for generating keys is replaced with another means for generating keys, but keys are still generated by the key-producing side. Note also that while Kaufman discloses use of a message digest algorithm to produce a new key from an old key, he does not necessarily limit the types of message digest algorithms that could be used. The trap-door function disclosed by Schneier is a type of message digest/hashing algorithm, thus it would have been obvious to one of ordinary skill in the art to at least try to use the trap-door algorithm disclosed by Schneier the specific message digest/hashing algorithm to derive a new key from an old key because it is nothing more than applying a known technique to a known device ready for improvement to yield predictable results.

Claims 10-11 and 25-26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Candelore (US 6,363,149).

Claims 10 and 25:

Candelore does not explicitly disclose wherein said key-issuing server and said provider of protected data are integrated. However, the examiner submits that it would have been obvious to have these items be integrated as one unit in Candelore's invention because as per MPEP 2144.04(V)(B), it is obvious to make separate structures integral.

Claims 11 and 26:

Candelore further discloses wherein said one-way key derivation function is implemented in a device on the key-consuming side for generating key information of said at least one older key generation from key information of the new key generation (col 9, line 25-col 10, line 27 and Fig 5A).

Candelore does not explicitly disclose that the generating is done provided that additional data in the form of a predetermined access code is applied to the key derivation function. However, official notice is taken that hash functions which requires entry of a correct pin to properly generate the correct hash value were well known in the art at the time applicant's invention was made. It would have been obvious to one skilled in the art to modify Candelore's invention according to the limitations recited in claims 11 and 26. One skilled would have been motivated to do so because incorporating a pin into the calculation of a hash/key value increases the complexity of the hash, which would lead to stronger keys.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to PONNOREAY PICH whose telephone number is (571)272-7962. The examiner can normally be reached on 9:00am-4:30pm Mon-Thurs.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Ponnoreay Pich/
Examiner, Art Unit 2435